Please amend Claim 5 as shown below. The claims, as pending in the subject application, read as follows:

~~1. (Original) A method for the secure printing of print data from a client~~ application residing on a data network to a set top box which has a printer, said set top box residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

determining whether a secure communication path exists between said client application and said set top box;

transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said set top box; and

sending said print data from said set top box to said printer for printing.

2. (Original) A method according to Claim 1, wherein the step for determining whether a secure communication path exists between said client application and said set top box includes the use of a secure protocol between said client application and said cable head end, and between said cable head end and said set top box.

3. (Original) A method according to Claim 2, wherein the step for determining whether a secure communication path exists between said client application and said set top box further includes a confirmation through said secure protocol, that said

cable head end is a secure location, and a confirmation, through said secure protocol, that said set top box is a secure location.

4. (Original) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said set top box includes sending said print data from said client application to said cable head end in a device-independent format, transforming said print data from said device-independent format to a rasterized format which corresponds to said printer, and then sending said print data in said rasterized format from said cable head end to said set top box for printing on said printer.

5. (Currently amended) A method according to Claim 1, wherein the ~~step~~ set for transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said set top box includes encrypting said print data, sending said encrypted print data from said client application to said cable head end, sending said encrypted print data from said cable head end to said set top box, decrypting said print data, and sending the decrypted print data to said printer for printing.

6. (Original) A method according to Claim 3, wherein said confirmation that said set top box is a secure location is sent from said set top box to said cable head end.

-4-

7. (Original) A method according to Claim 3, wherein said confirmation that said cable head end is a secure location is sent from said cable head end to said client application.

8. (Original) A method according to Claim 1, wherein the step for transmitting, in response to a determination that said secure communication path exists, said print data from said client application to said set top box includes transforming, by said client application, said print data from said device-independent format to a rasterized format which corresponds to said printer, sending said print data in said rasterized format from said client application to said cable head end, and then sending said print data in said rasterized format from said cable head end to said set top box for printing on said printer.

9. (Original) A method according to Claim 2, wherein said secure protocol is a secure sockets layer protocol.

10. (Original) A method according to Claim 2, wherein the step for determining whether a secure communication path exists between said client application and said set top box includes the transmission of at least one certificate from said set top box to said cable head end and the transmission of at least one certificate from said cable head end to said client application.

11. (Original) A method for the secure printing of print data from a client application residing on a data network to a set top box which has a printer, said set top box residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

determining that a secure communication path exists between said client application and said cable head end upon receipt through a secure protocol of a confirmation from said cable head end that said cable head end is a secure location;

sending, in response to a determination that said secure communication path exists, said print data from said client application to said cable head end in a device-independent format;

transforming in said cable head end, said print data from said device-independent format to a rasterized format which corresponds to said printer;

determining that a secure communication path exists between said cable head and said set top box upon receipt, through a secure protocol, of a confirmation from said set top box that said set top box is a secure location; and

sending, in response to a determination that said secure communication path exists, said print data in said rasterized format from said cable head end to said set top box for printing on said printer.

12. (Original) A method for the secure printing of print data from a client application residing on a data network to a set top box which has a printer, said set top box residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said method comprising the steps of:

generating print data in said client application;

transforming, in said client application, said print data from said device-independent format to a rasterized format which corresponds to said printer;

encrypting, in said client application, said print data in said rasterized format;

sending said encrypted print data in said rasterized format from said client application to said cable head end;

sending said encrypted print data in said rasterized format from said cable head end to said set top box; and

decrypting, in said set top box, said print data in said rasterized format for printing on said printer.

13. (Original) An apparatus for the secure printing of print data from a client application residing on a data network to a set top box which has a printer, said set top box residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, comprising:

a program memory for storing process steps executable to perform a method according to any of Claims 1 to 12; and

a processor for executing the process steps stored in said program memory.

- 7 -

~~14. (Original) Computer-executable process steps stored on a computer~~ readable medium, said computer-executable process steps for the secure printing of print data from a client application residing on a data network to a set top box which has a printer, said set top box residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 12.

15. (Original) A computer-readable medium which stores computer-executable process steps, the computer-executable process steps to achieve the secure printing of print data from a client application residing on a data network to a set top box which has a printer, said set top box residing on a digital cable network which has a cable head end for interfacing said digital cable network to said data network, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 12.

- 8 -